



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools
and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security
Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

Water outage hits several eastern ND communities. Several eastern North Dakota communities experienced a water outage December 9. KSJB radio reported that Stutsman Rural Water District members north of Jamestown would have no water supply for much of the day while a water line break is repaired. The affected towns and areas are Pingree, Buchanan, Sutton, Bordulac, Courtenay, Edmunds, Carrington, Melville, and the Spiritwood Lake area. Source:

http://www.bismarcktribune.com/news/state-and-regional/article_3564a9ee-03b6-11e0-b487-001cc4c03286.html

REGIONAL

(Minnesota) Search warrant served on raw milk in Minnetonka. Minnesota agricultural officials confiscated hundreds of gallons of milk delivered to a house in the latest development of their crackdown on unpasteurized milk. Investigators December 7 confiscated about 400 gallons of milk a man was delivering to a house in Minnetonka, where customers were waiting to pick up their orders, according to search warrant documents cited by Minnesota Public Radio. The state has tried repeatedly to stop the man and his brother from selling unpasteurized milk. Agriculture officials towed the brothers' truck to a state building. The search warrant said officials received an anonymous tip the home had served as a raw milk drop site in the past. The man said he has a constitutional right to sell dairy products. State health officials have blamed the farm in Sibley County for illnesses associated with an E. coli outbreak earlier this year that sickened several people. State inspectors reported problems, including rodent droppings and possible manure contamination in the milking facilities. Source:

<http://www.grandforksherald.com/event/article/id/186364/group/homepage/>

(Minnesota) At least 40 treated for ammonia spill injuries. At least 40 people have been treated at hospitals following an ammonia spill that evacuated a small city in eastern Minnesota. Cannon Falls Medical Center said most of the 19 people treated due to injuries from the leak in Randolph will be released December 8. Twenty-one patients were treated at Northfield Hospital. It said five were admitted and one required decontamination. Dakota County emergency managers said a ruptured line spilled anhydrous ammonia at the River Country Co-op north of Randolph. The caustic chemical can cause respiratory injuries. The emergency preparedness coordinator said about 400 residents of Randolph were evacuated to a nearby fire station. Students from the school complex were sent to a church outside the city. Source: <http://www.wkbt.com/Global/story.asp?S=13638246>

(Montana) Grenade triggers evacuation at Easter Seals-Goodwill. A suspicious package delivered to Easter Seals-Goodwill in Great Falls, Montana, triggered the evacuation of nearly 100 people December 6. Just before 10 a.m., an item that looked like a grenade was found among the donations at the facility, located at 4400 Central Avenue. Great Falls police and the Explosive Ordnance Disposal team from Malmstrom Air Force Base were called in to investigate. The donated item was, in fact, a

UNCLASSIFIED

grenade, but it had been hollowed out. The grenade was taken by the Malmstrom EOD unit for disposal. Everyone was allowed back into the building by 11:30 a.m. Source:

<http://www.krtv.com/news/grenade-triggers-evacuation-at-easter-seals-goodwill/>

NATIONAL

(Florida) **Copper wire caper.** Police in Stuart, Florida, are looking for the culprits who stole copper wire. Sometime over the Thanksgiving break, a thief or thieves climbed the fence at the sewage treatment plant and stole heavy spools of copper wire. The wire is so thick no ordinary tools could cut through it. The crooks took advantage of a hole designed in the wall around the plant and rolled the wire through. "This took a lot of work to unbundle 1,500 pounds of copper wiring then load it on a vehicle to transport it away from the site," said a Stuart police sergeant. Police said they have put an alert out to area metal recyclers. The metal exchanges have copper trading at about \$3.80 per pound. Source: http://www.wptv.com/dpp/news/region_martin_county/stuart/copper-wirecaper-

INTERNATIONAL

Georgia arrests 6, calling them agents for Russia and accusing them of staging blasts. The Republic of Georgia arrested six people suspected of being agents for Russia and accused them of staging a series of explosions, including one outside the U.S. Embassy in the capital, officials said December 7. The deputy interior minister said the suspects were recruited by the Russian military. A series of spy flaps has aggravated tense relations between the two former Soviet republics. The deputy said the six people, four men and two women, are accused of staging an explosion outside the U.S. Embassy in September, that caused no injuries, and several other blasts, including a blast in November outside the Labor Party's offices in Tbilisi that killed a woman. The deputy said that the suspects, all of them Georgian citizens, were arrested over the weekend. She said authorities had confiscated explosives and weapons during searches at their homes. The deputy said that two other suspected members of the group were hiding in Georgia's Russia-backed breakaway province of Abkhazia. Source: <http://www.brandonsun.com/world/breaking-news/georgia-arrests-6-suspected-russian-agents-accused-of-staging-explosions-outside-buildings-111433254.html?thx=y>

Gunmen kill 4 in attack on 2 Mexico rehab centers. Mexican police said armed commandos attacked two drug rehabilitation centers in Ciudad Juarez, Mexico, across from El Paso, Texas, killing four people and wounding five. A municipal police spokesman said the attacks occurred December 5. Three were killed in one center and one was killed in another. Gangs have killed dozens in drug rehabilitation centers in the last 2 years across Mexico, including nine last summer in Durango in the north, and 19 in Chihuahua city, capital of the border state where Ciudad Juarez is located. Cartels run the centers in some cases to recruit addicts, leaving them open to attacks from rivals. Source: <http://www.google.com/hostednews/ap/article/ALeqM5jFbXWwg2kUiswnDVBF7E1fLj2vrg?docId=9c9c7dd5bdee4212b9293b3e5d74752f>

Thousands evacuated in Australian floods. Thousands of Australians were evacuated from their homes or stranded as surging floodwaters swamped towns in the area's worst deluge in 36 years, officials said December 6. Parts of south-eastern New South Wales were declared natural disaster areas as swollen rivers spilled into the streets and water levels continued to - 23 - rise, forcing the closure of major highways, the state premier said. "We are anticipating that there may be additional

UNCLASSIFIED

flooding and the water may still be rising here in Wagga and as we see over the next few days those floodwaters move westward,” he told reporters from the badly hit town. About 3,000 properties were isolated and around

1,500 had been evacuated, according to the State Emergency Service (SES). A total of 34 New South Wales regions were now natural disaster zones, the premier said, with 17 declarations issued in the past few days. About 170 soldiers had joined hundreds of SES volunteers in sandbagging and rescue efforts.

Source: <http://www.news24.com/World/News/Thousands-evacuated-in-Australianfloods-20101206>

BANKING AND FINANCE INDUSTRY

Chase merchant customers targeted in new phishing campaign. Security researchers warn of a new e-mail phishing campaign targeting customers of JPMorgan Chase’s payment processing and merchant services, Chase Paymentech. According to researchers from messaging security company AppRiver, the e-mails began hitting people’s in-boxes at an aggressive rate December 7. The message claims account information must be updated and provides users with a link to a phishing page. The page is hosted on domains of the form online13-chasepaymentech.com, whose names are close to the real chasepaymentech.com. A message on the fake page reads: “Welcome back! You may notice some changes to your login page, but your login process is still the same. We have made updates on our end in order to ease usability and maximize functionality.” If users input their usernames and passwords, they are taken to a form that asks for a wealth of personal information. Since Chase Paymentech is the payment processing and merchant services arm of JPMorgan Chase, it means that unlike most phishing attacks, this one targets businesses. Source:

<http://news.softpedia.com/news/Chase-Bank-Phishing-Campaign-in-Circulation-171184.shtml>

New PayPal phishing campaign in circulation. A new wave of PayPal phishing e-mails carrying a fake form allegedly intended for account information update purposes has been hitting people’s inboxes since December 8. The rogue e-mails purport to come from “PayPal.com” and bear a subject of “Your account has been temporarily limited !” The body contains the PayPal logo and a message instructing users to fill in and submit the attached form. The attached archive is called PayPal.com_Account_Confirmation_Form.pdf.zip and contains a file called PayPal.com_Account_Confirmation_Form.pdf.html. The double extension is meant to trick users on operating systems automatically hiding the known file extensions, like Windows Vista and 7, into thinking the file is a PDF document. When opened, the HTML displays a page that mimics the look and feel of the PayPal Web site and displays a form asking for personal and credit card information. The IP address suggests the server where phished information is stored is located in Iran. Source:

<http://news.softpedia.com/news/New-PayPal-Phishing-Campaign-in-Circulation-171491.shtml>

WikiLeaks supporters claim to have brought down MasterCard website. A group of hackers supporting the WikiLeaks organization claimed December 7 that it brought down the Web site of MasterCard. The credit card company recently cut the ability of funders to use MasterCard services to donate to WikiLeaks, as did a number of other firms, including rival Visa and online payment service Paypal. The attackers claimed on their Twitter account that the denial of service attack on the Web site was part of “Operation:Payback.” Mastercard.com was not accessible immediately following the announcement, and trying to log onto the site, users received a “Network Error” message. The same group of hackers claimed earlier the week of December 5 that they had managed to disrupt the Web

site of the Swiss Postfinance, a bank that shut the account of the WikiLeaks founder. Source: http://www.monstersandcritics.com/news/business/news/article_1604269.php/WikiLeaks-supporters-claim-to-have-brought-down-MasterCard-website

Zeus targets major retailers. Trusteer has discovered a Zeus botnet argeting credit card accounts of major retailers, including Macy's and Nordstrom just as the holiday gift buying season is in full swing. They captured and analyzed malware samples designed to steal credit card information, probably in order to conduct card-not-present (CNP) fraud. This attack is using a Zeus 2.1.0.8 botnet — the latest and most sophisticated version of the Zeus malware platform. CNP fraud refers to transactions when a credit card is not physically present, as in an Internet, mail or phone purchase. It is difficult for a merchant to verify the actual cardholder is indeed authorizing the purchase. Because of the greater risk, card issuers tend to charge merchants higher fees for CNP transactions. To make matters worse, merchants are typically responsible for CNP fraud transactions. Therefore, CNP merchants must take extra precaution against fraud exposure and associated losses. Source: http://www.net-security.org/malware_news.php?id=1559

Zeus-related fake electronic tax payment emails are back. Security researchers warn of a new wave of fake Electronic Federal Tax Payment System (EFTPS) e-mails directing users to drive-by download Web sites that distribute the Zeus banking Trojan. The fake e-mails claim the recipient's electronic tax payment was rejected due to a error in the submission form. They read: "Your Federal Tax Payment ID: ##### has been rejected. [where # is a digit] Return Reason Code R21 - The identification number used in the Company Identification Field is not valid. Please, check the information and refer to Code R21 to get details about your company payment in transaction contacts section: <http://eftps.gov/R21> In other way forward information to your accountant adviser. EFTPS: The Electronic Federal Payment System PLEASE NOTE: Your tax payment is due regardless of EFTPS online availability. In case of an emergency, you can always make your tax payment by calling the EFTPS." It seems the attack targets businesses that would be forced to use EFTPS as default tax payment method starting from January 2011. According to security researchers from M86 Security, who analyzed the e-mails, the included link takes users to an attack page that tries to exploit vulnerabilities in outdated versions of Java and Adobe Reader. In particular, the exploit pack targets four vulnerabilities in Java and one in Adobe Reader. Successful exploitation of any of them results in a variant of the Zeus banking Trojan being installed on the system. Source: <http://news.softpedia.com/news/Zeus-Related-Fake-Electronic-Tax-Payment-Emails-Are-Back-170853.shtml>

Fake Google and Facebook joint prize campaign leads to Zbot. Security researchers warn spam e-mails suggesting a joint prizes giveaway campaign from Google and Facebook eventually lead to a variant of the Zbot banking Trojan. The fake e-mails purport to come from "Google and Facebook team." The message suggests Google and Facebook, have decided to join together to give prizes away to users. The e-mails read: "Dear subscriber, As you may know, the holidays are just around the corner, so all of us here at Google and Facebook decided to come together and bring you a new contest with lots of prizes, including, but not limited to, the new Google Chrome OS which will be released in January 2011, Nexus One smartphones, Google Maps GPS for your favourite mobile phone and lots more. Think of it as our way of saying: 'Thank you!' for supporting our work all this time. For a chance to win, all you have to do is go to the attached page and follow the instructions. Hope you enjoy, Google & Facebook." Two of the three mentioned prizes are actually free products,

UNCLASSIFIED

and all are from Google. The attached file is called "Google & Facebook.html" and contains obfuscated JavaScript code. When opened inside a browser it redirects to a Web site that serves an exe file. According to BitDefender security researchers, the file is a trojan downloader written in .NET that requires the .NET Framework installed on the targeted system in order to run. The original dropper installs a secondary downloader that distributes several information stealing Trojans, including Zbot. Source: <http://news.softpedia.com/news/Fake-Google-and-Facebook-Joint-Prize-Emails-Lead-to-Zbot-170972.shtml>

'Operation Broken Trust' targets financial fraud. A nationwide law enforcement crackdown targeting financial fraud has led to cases against 343 criminal defendants involving \$8.3 billion in estimated losses, the U.S. Attorney General announced December 6. "Operation Broken Trust" is - 6 - the first national effort of its kind aimed at a broad array of investment fraud schemes, and the 3 and one-half month campaign was organized by the Presidential administration's Financial Fraud Enforcement Task Force. The schemes that were uncovered highlight "the pervasiveness of the threat," the FBI's Executive Assistant Director told a news conference. In one case in Texas, an oil and gas investment Ponzi scheme defrauded 7,700 investors of more than \$485 million. In another case, in Chicago, Illinois, the operator of a Ponzi scheme victimized elderly Italian immigrants and hundreds of others after promising them annual returns of 10 to 15 percent.

Source:

<http://www.washingtonpost.com/wpdyn/content/article/2010/12/06/AR2010120602898.html?hpid=moreheadlines>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Vermont) NRC issues new rules for buried cables. The Nuclear Regulatory Commission (NRC) announced new rules December 7 regarding submerged cables at all nuclear plants. Based on a recent review, NRC staff identified 269 cable failures at nuclear facilities across the country, including 65 sites and 104 reactor units a spokesman for the NRC wrote in an e-mail. NRC staff stated cable failures have a variety of causes, including manufacturing defects, damage caused by shipping and installation, and exposure to electrical transients or abnormal environmental conditions during operation. The likelihood of failure from any of these factors increases over time as the cable insulation degrades and/or is exposed to water, the document states. "The submerged electrical cable issue is not that the cables fail immediately, it's that the moisture causes the cable insulation to degrade faster than expected, leading to shorter service lifetime," director of nuclear safety project for the Union of Concerned Scientist wrote in an e-mail. Vermont Yankee is one of the plants to experience cable submergence, the spokesman wrote. Source:

http://www.reformer.com/ci_16803140?source=most_viewed

COMMERCIAL FACILITIES

(Washington) 'Dummy bomb' causes Mount Vernon strip mall evacuation. Police said a suspicious package that forced them to evacuate a strip mall in Mount Vernon, Washington, December 9 had all the makings of a bomb, but it was not set up to detonate. The manager of the Dollar Tree store at 220 E. College Way called 911 around 5 p.m. after spotting the package with wires coming out of it. Police evacuated nearby businesses and brought in the bomb squad. For a time, police said they believed the package may have been an actual bomb and they planned to blow it up. Upon closer

UNCLASSIFIED

UNCLASSIFIED

inspection, they determined it was a dummy bomb. They said it contained shrapnel, wires and a battery, but there was no way to detonate it. Source: <http://www.king5.com/news/local/Bomb-squad-responds-to-suspicious-package-in-Mount-Vernon-111640949.html>

(Wisconsin) 2 people arrested after 6-hour freeway standoff. Two people have been arrested following a 6-hour standoff that shut down a Milwaukee, Wisconsin freeway. The situation began about 4 a.m. December 10 when a male driver and female passenger refused deputies' commands to leave a suspected stolen SUV on westbound Interstate 94. At about 10 a.m., tactical officers used a robot to break a window in the vehicle and send a cloud of gas inside. That is when the driver opened the front door, held his hands up and laid down on the freeway. Deputies removed the passenger from the vehicle. Authorities have not said whether the suspects were armed or why they refused to come out of the SUV. Traffic on the major thoroughfare was shut down during the morning commute. Source: <http://www.kivitv.com/Global/story.asp?S=13651355>

(Hawaii) Discovery of 81 mm mortar round closes streets in Makiki. A passerby discovered an unexploded World War II mortar round in a plastic bag in a trash can at Cartwright Field in Makiki, Hawaii, December 7, causing police to close off streets in the area for about an hour. The Honolulu Police Department's bomb squad was dispatched to the city park after a man reported finding the potential explosive device at 8:50 a.m. Police closed Lunalilo Street between Keeaumoku and Kewalo streets, Keeaumoku Street from Beretania Street to Wilder Avenue, and Kinau Street from Keeaumoku Street to Makiki Street until the device was removed. The 81 mm mortar round was taken to Schofield Barracks for disposal by Army ordnance experts and the roads re-opened at 10 a.m., police said. The device was destroyed by soldiers from the 706th Explosive Ordnance Detachment assigned to the 45th Sustainment Brigade. Source: <http://www.staradvertiser.com/news/breaking/111546784.html>

COMMUNICATIONS SECTOR

Hacker brings enhanced security to jailbroken iPhones. A computer consultant is adding a security measure known as ASLR to iPhones to make them more resistant to malware attacks. Short for address space layout randomization, ASLR has been absent from all iOS devices since their inception, making possible the types of attacks that commandeered a fully patched iPhone at the Pwn2Own hacker contest. By randomizing the memory locations where injected code is executed, ASLR aims to thwart such exploits by making it impossible to know ahead of time where malicious payloads are located. Starting with Windows Vista, Microsoft has baked ASLR into its operating system, and the recently released mobile version of Windows 7 is also endowed with the protection, said the principal security analyst at Independent Security Evaluators, who cited private conversations with Microsoft engineers. By comparison, Apple has built only limited ASLR into Mac OS X and has left it out of iOS altogether. At a conference scheduled for the week of December 13, a security consultant and application developer for Germany-based SektionEins, plans to unveil a process for jailbreaking iDevices that automatically fortifies them with ASLR. It works by reordering the contents of dyld_shared_cache, a massive file that houses the libraries. Source: http://www.theregister.co.uk/2010/12/07/enhanced_iphone_security/

UNCLASSIFIED

CRITICAL MANUFACTURING

Qantas A380 engine had problems before explosion. It has been revealed that the engine that disintegrated on a Qantas Airbus A380 near Singapore in November had earlier been taken off the aircraft to fix another problem. The Australian newspaper said investigators have revealed the engine was only refitted in February 2010. An Australian Transport Safety Bureau report released the week of November 29 shows the No. 2 engine was originally fitted as the aircraft's No. 4 engine but was removed last year after metal was found in a chip detector. The relatively new engine had performed just 3,419 flight hours and 416 landing and take-off cycles at the time. The engine was sent to a Singapore workshop certified to maintain and repair Rolls-Royce engines in September 2009. Engineers found spalling in a low-pressure compressor bearing and replaced the bearing assembly. The low-pressure compressor is a different part of the engine than the one - 5 - that failed in the dramatic Singapore incident. The repair was completed in December 2009. The engine was fitted to the aircraft February 24 and had completed a further 2,895 flight hours since then, the report said.

Source: <http://www.smh.com.au/travel/travel-news/qantas-a380-engine-had-problemsbefore-explosion-20101206-18mbp.html>

DEFENSE/ INDUSTRY BASE SECTOR

U.S. agents raid offices of Afghan, Iraq security contractor. Federal agents raided the Tennessee headquarters of a security contractor involved in Afghanistan and Iraq December 8 on warrants officials said were related to alleged violations of defense-related export controls. The contractor, EOD Technology Inc. (EODT), provides security and other services for the State and Defense departments. It was selected in late September to take over security for the U.S. Embassy compound in Kabul. One federal official said the alleged offenses fell under a law known as International Traffic in Arms Regulations, which governs export and import of certain defense-related items. The raid, directed by the U.S. attorney for eastern Tennessee, included agents from Immigration and Customs Enforcement, DHS, the FBI, and the Defense Criminal Investigative Service. Court documents were sealed and law enforcement officials said they would make no public comment on what they described as an ongoing investigation begun more than 1 year ago by the Special Inspector General for Iraq Reconstruction. EODT has been cited in the past for activities deemed "at odds with with U.S. interests in the region," according to the U.S. Senate Foreign Relations Committee. Source:

<http://www.washingtonpost.com/wp-dyn/content/article/2010/12/09/AR2010120907072.html>

(Tennessee) EOD Technology offices raided by feds. A team of special agents raided a pair of office buildings operated by EOD Technology December 8 in Lenoir City and Roane County, Tennessee. EOD Technology is a private security contractor that does millions of dollars in business with the U.S. Department of Defense in Iraq and Afghanistan. None of the agencies involved, including the United States Attorney's office will comment as to what exactly they are investigating. The two searches are just the latest for what has been a bad couple of months of publicity for the East Tennessee based contractor. A few months back, the United States Senate Armed Services Committee found that EOD Technology and other private security contractors relied on Afghani strongmen to fulfill taxpayer paid contracts. Source: <http://www.wbir.com/news/article/146867/2/EOD-Technology-offices-raided-by-feds>

UNCLASSIFIED

(Florida) SpaceX rocket, capsule launched in test for commercial space industry. The first of what NASA hopes will someday be a fleet of privately built rockets and capsules to supply the international space station launched from Cape Canaveral, Florida, December 8 in a major test for the commercial space industry. If all goes well, the capsule will circle the globe twice and then splash down 90 minutes later in the Pacific Ocean. The first attempt to launch at about 9:15 a.m. was aborted after an indicator falsely reported a problem 13 minutes from takeoff, and the launch took place 90 minutes later. The Falcon 9 rocket built by Space Exploration Technologies Corp., or SpaceX, is on its first full test flight. The flight is an important moment for the President and his administration's hopes to expand commercial space efforts in low-Earth orbit as a way to free up NASA funds for missions to send astronauts much deeper into space and ultimately to Mars. Source:

<http://www.washingtonpost.com/wp-dyn/content/article/2010/12/08/AR2010120801591.html?hpid=topnews>

Charge: Woodinville man tried to send military equipment to China. Federal prosecutors have brought charges against a 46-year-old man from Woodinville, Washington, accused of smuggling military equipment to China. The suspect was arrested December 3 after nearly 2 years of investigation by the FBI. He is purported to have attempted to send 300 satellite components to China. He allegedly told an informant the parts were meant for the China Space Technology Co.'s spacecraft program. On another occasion, federal investigators contend the suspect said some of the parts would be used in the design of "China's new generation of passenger jet." Prosecutors contend he agreed to pay \$620,000 to obtain the parts. The suspect is charged with conspiracy to violate federal arms control laws, which carries a maximum term of 5 years in prison. Source:

<http://blog.seattlepi.com/seattle911/archives/230765.asp>

EMERGENCY SERVICES

(Illinois) Bomb threat at Madison County Criminal Justice Center. A bomb threat was made against the criminal justice center in Madison County, Illinois, but the threat was ultimately deemed non-existent. According to the chief of detectives for the Madison County Sheriff's Office, the threat was made for a specific time for December 6. The investigation was launched at 2 p.m. The Madison County Criminal Justice Center was evacuated while authorities conducted their search. A bomb certified canine unit was dispatched to the building. But in the end, the building was deemed safe. A potential suspect was identified and taken into custody. The case was slated to be presented to the state attorney's office for formal charges on December 7. Source:

<http://www.ksdk.com/news/local/story.aspx?storyid=231514&catid=3>

ENERGY

(Illinois) Massive oil pipeline to be checked for defective steel. TransCanada Corp. is digging up 10 sections of a new, \$5.2 billion crude oil pipeline after government-ordered tests identified possibly defective steel that may have been used in its construction. As one of the longest and most expensive pipelines ever built in North America, the Keystone pipeline can carry about a half-million barrels per day, enough to supply about 2 percent of the country's daily demand. Oil began reaching the refinery in late June and will continue to flow during the work. Federal regulators ordered more extensive tests on the Keystone line after problems with substandard steel surfaced in several other projects. An investigation revealed several pipelines built during a construction boom from 2007 to 2009

UNCLASSIFIED

UNCLASSIFIED

contained significant amounts of defective pipe that stretched under pressure. TransCanada officials declined to provide details about the 47 anomalies they found, including the percentage of any expansions. Nine anomalies were detected in Missouri, 12 in Kansas, 14 in Nebraska and 12 in South Dakota. Investigators traced the problems to defective steel produced by several mills, but mostly by Welspun Power and Steel, a manufacturer based in India. The Keystone pipeline stretches 2,151 miles from the Athabasca tar sands of Alberta, Canada to the ConocoPhillips' Wood River refinery in Roxana, Illinois, then on to Patoka, Illinois. Source:

<http://www.istockanalyst.com/article/viewiStockNews/articleid/4734390>

(Ohio) Morrow County power outages blamed on copper thefts. About 1,200 American Electric Power customers in Mount Gilead, Ohio lost power December 8 because of problems at a substation caused by copper thieves. An American Electric Power (AEP) spokeswoman said it appeared someone cut through a fence and stole copper grounds from a substation on County Road 24 in Fulton, Ohio. The spokeswoman said replacement equipment was needed to fix the problem. It could take up to 6 hours to restore power to all customers, AEP said. Highland West Elementary School in the Highland Local School District was closed December 8 because of the outage. Source:

<http://www.10tv.com/live/content/local/stories/2010/12/08/story-morrow-county-power-outages-copper-thefts.html?sid=102>

FOOD AND AGRICULTURE

(Florida) Pathogen continues to threaten Florida's \$9-B citrus industry. An insect-borne bacterial disease ravaging Florida's citrus crop means the juice squeezed from the Sunshine State's fruit may soon come from trees that have had their genetic makeup modified. The blight, commonly known as "greening," is the world's most destructive citrus disease. GMO juice would likely be reviled by biotech industry critics. But a scientist with the U.S. Department of Agriculture, and other experts said there may be no other choice in the battle against greening. "It's the most serious disease threat that the Florida citrus industry has ever faced," he said. Most scientists who have studied the problem seem to agree genetic modification, and the cultivation of trees resistant to the bacteria that causes "greening" disease, currently hold out the only real long-term hope of fighting it. That was the conclusion of a report sponsored by the Florida Department of Citrus and US National Academy of Sciences in March, which highlighted the need for urgency to save Florida's \$9-billion citrus industry. Source: <http://www.bworldonline.com/main/content.php?id=22579>

(California) California firm recalls raw and ready-to-eat pork products. L&R Fine Fashions, Inc., a Garden Grove, California, establishment, is recalling approximately 2,182 pounds of raw pork paste and ready-to-eat fried pork loaf products because they contain an undeclared allergen, wheat, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced December 8. Wheat is a known allergen, which is not declared on the label. The products subject to recall include: 11-ounce packages of "Kim Loan Gio Song Pork Paste Fish Sauce Added" and 14-ounce chubs of "Kim Loan Cha Chien Fried Pork Loaf Fish Sauce Added." Each product bears the establishment number "Est. 40074" inside the USDA mark of inspection. The products subject to recall were produced between January 22, 2010 and December 6, 2010. These products were distributed to retail establishments in Southern California. Source:

http://imperialvalleynews.com/index.php?option=com_content&task=view&id=8817&Itemid=1

UNCLASSIFIED

UNCLASSIFIED

(California) Atlas walnut company recalls walnuts for Salmonella risk. Atlas Walnut Co. of California announced a voluntary recall of walnut halves and pieces due to the risk of Salmonella contamination. The recall was made after Azar Nut Company, which receives product from Atlas, asked U.S. Foodservice to recall the products after a shipment tested positive for Salmonella. No illness have been reported thus far. Azar reported their own tests for Salmonella are negative, but they are nevertheless initiating the recall in an excess of caution. Source: [http://www.foodpoisonjournal.com/2010/12/articles/foodborne-illness-outbreaks/atlas-walnut-company-recalls-walnuts-for-salmonella-risk/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+FoodPoisonBlog+\(Food+Poison+Blog\)](http://www.foodpoisonjournal.com/2010/12/articles/foodborne-illness-outbreaks/atlas-walnut-company-recalls-walnuts-for-salmonella-risk/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+FoodPoisonBlog+(Food+Poison+Blog))

(California) 42,000 pounds of tamales recalled. Diana's Mexican Food Products in California is recalling 42,000 pounds of chicken tamales because the label does not say the tamales contain whey. The U.S. - 11 - Department of Agriculture's (USDA's) Food Safety and Inspection Service (FSIS) announced December 3 it had done what department called a routine inspection at the South Bay company's plant. USDA officials said whey is a known allergen and it must be declared on the label. There are no reports of anyone becoming sick from the tamales, and if a person is not allergic to whey, the tamales are perfectly safe to eat. The tamales were produced between February 2010 and December 2, 2010 and were distributed to restaurants in California. Source: <http://www.ktla.com/news/landing/ktla-tamales-recalled,0,1819144.story>

72,000 pounds of canned chicken salad recalled. The discovery of hard plastic inside packages prompted a nationwide recall of 72,000 pounds of canned chicken salad, one of several recalls involving poultry and meat products issued through U.S. food safety authorities in recent days. The Suter Company is recalling 8.2-ounce packages of the "Bumble Bee Lunch on the Run Chicken Salad Complete Lunch Kit," and 3.5-ounce packages of "Bumble Bee Chicken Salad with Crackers," according to a statement released December 5 by the U.S. Department of Agriculture's Food Safety and Inspection Service. While the company is headquartered in Sycamore, Illinois, its products are sold from coast to coast. The recalled products — which have a August 2011 "best-by" date for the lunch kit, and February 2012 corresponding date for the cracker package — were put together and shipped out to distributors and stores between August 14 and 28 of 2010. Source: <http://www.cnn.com/2010/HEALTH/12/05/chicken.recall/index.html?hpt=T2>

(Ohio) Apple cider recalled in Ohio. Bauman Orchards, Inc. of Rittman, Ohio, recalled approximately 50,000 gallons of apple cider after an Ohio Department of Agriculture inspection discovered potential product contamination. The vice president of the company said the recall was a precautionary measure because the apple cider was underprocessed. He said no illnesses or adverse effects have been reported to the company in connection with the cider. The cider can be identified by: UPC 2290600128 gallons, UPC 2290600064 half gallons. Manufacture dates are September 1, 2010, through December 5, 2010. The cider was distributed to stores in Ohio. Source: <http://www.foodsafetynews.com/2010/12/apple-cider-recalled-in-ohio/>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

US: Hackers hit universities' database 'jackpots'. Since 2008, 158 data breaches have compromised more than 2.3 million records at American higher education institutions, according to a recent report by Application Security, Inc, a U.S. database safety company. Identity theft has become the U.S.' largest consumer complaint, according to the Federal Trade Commission (FTC), with nearly 1 million new victims each year. The problem has been exacerbated — and the illicit rewards made greater — by cyber criminals successfully hacking into the databases of semi-autonomous tertiary educational institutions. "When an attacker gets access to university databases, it's like hitting the jackpot," said the New York-based Application Security's vice-president of product management. For larger institutions, with tens of thousands of students along with staff and faculty, "a university or college could be housing potentially billions of PII (personally identifiable information)," he said. Source: <http://www.universityworldnews.com/article.php?story=20101208202734901>

(Michigan) Homemade explosive brings bomb squad to downtown Howell. The Howell Police Department in Michigan dispatched officers to the area near the Howell Carnegie District Library at 314 W. Grand River Ave. on a report of a possible bomb in a parked vehicle at 8:15 p.m. December 7. Two Howell females contacted officers and drew their attention to a 1995 Nissan Maxima in the parking area on Chestnut Street to the west of the library, police said. One of the females said her estranged boyfriend, who is in jail on unrelated charges, had been putting together homemade explosive devices at their house in the 600 block of McCarthy Street. After the couple split up, she told police, she had packaged up those materials and put them in the car so she could take them to the police station and get them out of her house. The ex-girlfriend and the other female decided on the way to the station that it would be better to park the car and call police to pick up the materials. Howell police blocked off roadways around the library and contacted the bomb squad, which arrived at the scene at 9 p.m. The squad determined a homemade explosive device was among the items in the package and detonated the device at the scene without any injuries or property damage, police said. A state police robot could be seen taking what appeared to be a backpack away from the vehicle. Source: <http://www.livingstondaily.com/article/20101208/NEWS01/101208003/Homemade-explosive-brings-bomb-squad-to-downtown-Howell-with-additional-scene-photos->

(Arkansas) Seven counties to benefit from biometrics technology. On December 7, U.S. Immigration and Customs Enforcement (ICE) began using a federal information sharing capability in 7 additional Arkansas counties that helps federal immigration officials use biometrics to identify aliens, both lawfully and unlawfully present in the United States, who are booked into local law enforcement's custody for a crime. Previously, biometrics taken of individuals charged with a crime and booked into custody were checked for criminal history information against the Department of Justice's (DOJ) Integrated Automated Fingerprint Identification System (IAFIS). Now, through enhanced information sharing between DOJ and the DHS, biometrics submitted through the state to the FBI will be automatically checked against FBI criminal history records in IAFIS and biometrics-based immigration records in DHS's Automated Biometric Identification System. If fingerprints match those of someone in DHS' biometric system, the new automated process notifies ICE. ICE evaluates each case to determine the individual's immigration status and takes appropriate enforcement action. The announcement includes Crawford, Garland, Jefferson, Saline, Sebastian, Union, and White counties.

UNCLASSIFIED

ICE is now using this capability in 10 Arkansas jurisdictions. ICE is using this capability in 831 jurisdictions in 34 states. Source: <http://www.katv.com/Global/story.asp?S=13633336>

(Maryland) Baltimore arrest over 'recruitment center bomb plot'. Authorities have arrested a man in Baltimore, Maryland, for allegedly plotting to blow up a military recruitment center. A Department of Justice (DOJ) spokesman said the suspect was an American citizen. The spokesman said the man had been monitored by law enforcement officers for months as part of a sting operation. The U.S. Attorney's Office for Maryland said the suspect was plotting to blow up a military base using a vehicle bomb. The office added there was no danger to the public, and that the explosives were inert. It is not yet clear which of the military recruiting bases in Catonsville, Maryland was his alleged target. Source: <http://www.bbc.co.uk/news/world-us-canada-11953514>

(Georgia) Explosive found near MCLB. Officials with Marine Corps Logistics Base (MCLB) in Albany, Georgia, have confirmed that explosive materials were found inside a tactical vehicle near the installation's truck gate December 3. An MCLB Albany spokesman said that an investigation has been launched to determine both how the explosives found their way to the location and exactly what the explosives were. In a statement, a spokesman said that around 5:35 p.m. December 3, base officials discovered the explosives inside what they called a "tactical vehicle," located near the MCLB's truck gate. The area was secured and the material has been taken to an "isolated and safe area." Small scale evacuations of the immediate area were ordered and no one was injured, officials said. Source: http://www.albanyherald.com/news/headlines/Explosive_found_near_MCLB_111403104.html?ref=104

(Arkansas; Washington) Ark. man arrested in Seattle in bomb case. A 40-year-old Arkansas man has been arrested in Seattle, Washington, in connection with an attempted bombing of a polling place at a northwest Arkansas church in June, according to federal authorities. A U.S. attorney said the suspect was arrested without incident December 3, and appeared before a federal judge in Washington. He was ordered detained and returned to Arkansas. Court documents said the suspect was arrested on complaints of attempted use of force against those engaged in federally protected activities and possession of an unregistered firearm. Authorities found an improvised explosive device inside a 12-ounce soda can at Osage Baptist Church in Osage, Arkansas, June 8 and said that the bomb could have killed anyone within 10 to 15 feet of it had it exploded. An FBI Special Agent said authorities determined the device was powered by several AAA-size batteries that had their skins stripped off of them. In November, contractors cleaning out a foreclosed Huntsville residence once owned by the suspect found printed material that described the making of explosive devices and alerted authorities, who also found books and manuals related to constructing explosive devices and militia extremism, the FBI Special Agent said. He said authorities later found other bomb-making materials.

Source: http://www.seattlepi.com/local/6420ap_ar_church_bomb_arrest.html

Espionage investigation centers on Fort Bragg. A U.S. Navy intelligence specialist stationed at Fort Bragg in Fayetteville and Spring Lake, North Carolina, is under investigation for espionage after he sold top secret documents to an undercover FBI agent posing as a foreign intelligence officer, according to a search warrant filed in federal court December 3. A Naval Criminal Investigative Service spokesman (NCIS) said the 22-year-old, of the Naval Reserve, was being held in Norfolk, Virginia. The warrant indicated the suspect sold documents on several occasions staged by

UNCLASSIFIED

investigators at two Spring Lake hotels. According to the search warrant, the suspect met an undercover FBI agent November 15 in the lobby of the Hampton Inn on Bragg Boulevard. Posing as a foreign intelligence officer, the special agent brought the suspect to his room, where the suspect discussed his access to military computer networks and classified networks, the warrant noted. The suspect allegedly said he could be a very valuable source of information over the course of his planned 20-year Navy career. At a meeting the next day at the same hotel, the suspect produced two documents - one labeled "secret" and the other "top secret" and accepted \$1,500 in cash, the warrant alleged. He agreed to meet the agent again November 19, when he produced 51 pages of secret and top secret documents, according to the warrant. Source: <http://www.thesunnews.com/2010/12/05/1850907/espionage-investigationcenters.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Pro-WikiLeaks cyber army gains strength; thousands join DDoS attacks. The retaliatory attacks by pro-WikiLeaks activists are growing in strength as hackers add botnets and thousands of people download an open-source attack tool, security researchers said December 9. In recent days, distributed denial-of-service (DDoS) attacks have been launched against several sites, including those belonging to Amazon, MasterCard, PayPal, and the Swiss payment transaction firm PostFinance, after each terminated WikiLeaks accounts or pulled the plug on services. Most of those participating in the attacks are using the LOIC (Low Orbit Ion Cannon) DDoS tool, said researchers with Imperva and Sophos. The open-source tool, which is sometimes classified as a legitimate network- and firewall-stress testing utility, is being downloaded at the rate of about 1,000 copies per hour, said the Web research team lead at Imperva's Application Defense Center. LOIC has become the DDoS tool of choice in the pro-WikiLeaks attacks because users can synchronize their copies with a master command-and-control server, which then coordinates and amplifies the attacks. Source: http://www.computerworld.com/s/article/9200659/Pro_WikiLeaks_cyber_army_gains_strength_thousands_join_DDoS_attacks

Fake receipt program targets Amazon retailers. Amazon retailers are being targeted by fraudsters who have created a custom-built program that generates fake receipts for nonexistent orders, according to researchers from GFI Software. The program is designed to create a customized HTML file that closely resembles an actual Amazon.com receipt, wrote the senior threat researcher. A fraudster can fill out the date, item, price, order number, and address among other information. Users also have the option of selecting specific Amazon portals, including ".com," ".co.uk," ".fr," and ".ca." When the "generate" button is clicked, a file is placed in the computer's program folder which is nearly identical to the "printable order summary" on a legitimate receipt. The scam relies entirely on social engineering, with the fraudster hoping a vendor will be tricked into thinking a product was sold. Source: http://www.computerworld.com/s/article/9200601/Fake_receipt_program_targets_Amazon_retailers

Fake Facebook toolbar leads to malware. A new e-mail campaign initiated by spammers tries to take advantage of Facebook changes and lure users into downloading malware. This latest spam run offers a "Facebook toolbar". If the e-mail looks familiar, it is because it is identical to one used in a spam campaign more than half a year ago, when the offered file presented a veritable jumble of incongruous information. This time, the "Download Here" button takes the victim to a Web site

UNCLASSIFIED

where an automatic download of a file called fb.exe is started. According to Trend Micro researchers, it contains several component files, among which is a backdoor Trojan that installs an IRC client on the infected machine. Source: http://www.net-security.org/malware_news.php?id=1562

WikiLeaks-related spam carries worm. Malware pushers are taking advantage of users' curiosity about WikiLeaks to gain access to their computers. An e-mail with "IRAN Nuclear BOMB!" in the subject line has been detected by Symantec, with a spoofed header to make it look like it came from WikiLeaks.org, saying "OBAMA is and IMPOSTOR!" and offering an URL. By clicking on it, the victim is taken to a site where a Wikileaks.jar file attempts to download a worm on the victim's computer. The worm in question opens a backdoor into the system by using a predetermined port and IP address, and allows the attacker to do all kinds of mischief: stealing, spying, routing traffic through the computer. It can also spread further by copying itself to removable drives and the share folders of file-sharing programs. Source: http://www.net-security.org/malware_news.php?id=1560

Twitter hit by Goo.gl worm. Twitter has been hit with a new kind of worm exploiting Google's URL shortening service "goo.gl". According to TechCrunch, the Twitter virus is using links that start with "http://goo(dot)gl" in order to spread malware. In many cases, the message accompanying the infected link says that the user has "just found the easiest way to track who follows and unfollows you". The virus, which seems to have originated from Twitter's mobile site, tries to redirect unsuspecting users to malicious Web sites by encouraging them to click on the link. Using social engineering, users are fooled into thinking the link is secure based on the senders' reputation and the idea that URL belongs to a trusted Web giant. People are advised not to click on a random link, even if they have received it from a trusted source. Source: <http://www.itproportal.com/2010/12/8/twitter-hit-google-worm/>

Whitehats peer into new botnet's heart of 'Darkness' DDoSes R Us. Whitehat hackers are tracking a new botnet that has become a popular platform for launching Web attacks. Over the past few weeks, members of the Shadowserver group have observed the Darkness botnet unleashing distributed denial of service attacks on more than 100 Web sites in the financial, insurance, and retail industries. They have also uncovered an online campaign advertising DDoS-for-hire services that boast high quality and an average cost of \$50 for 24 hours of use. "It now appears that 'Darkness' is overtaking BlackEnergy as the DDoS bot of choice," a Shadowserver volunteer wrote. "There are many ads and offers for DDoS services using 'Darkness.' It is regularly updated and improved and of this writing is up to version 7. There also appear to be no shortage of buyers looking to add 'Darkness' to their botnet arsenal." Source: http://www.theregister.co.uk/2010/12/07/darkness_botnet/

Rogue private messages direct Facebook users to Waledac Trojan. A wave of rogue private messages received by many Facebook users directs them to malicious Web sites serving a version of the Waledac Trojan. According to scam tracking Web site Facecrooks, the messages read "I got you a surprise www.[random_name].blogspot(dot)com." Several different blogspot URLs were observed in these messages, suggesting the people behind this campaign have registered many accounts in advance and rotate them as soon as they get suspended. Visiting the Web sites triggers a prompt that reads "Download photoalbum" and serves an executable file called photo.exe, which is actually a Waledac variant. According to Symantec, Waledac "is a worm that spreads by sending emails that contain links to copies of itself. It also sends spam, downloads other threats, and operates as part of a botnet." In its description of the threats, the antivirus vendor said Waledac authors commonly

UNCLASSIFIED

organize social engineering-based campaigns to trick users into installing it. Source:

<http://news.softpedia.com/news/Rogue-Private-Messages-Direct-Facebook-Users-to-Waledac-Trojan-171183.shtml>

NATIONAL MONUMENTS AND ICONS

(Hawaii) Pearl Harbor Visitors Center evacuated after suspicious bag found. There was a bit of drama December 6 at the new Pearl Harbor Visitors Center in Hawaii. Around 10:45 a.m. authorities discovered a duffel bag with a suspicious object inside. They fully evacuated Building G of the newly opened visitors center while federal authorities investigated. "We evacuated the gallery, secured the perimeter, and basically looked for the owner and tried to identify what was within that bag. And so, until we completed that we actually had to keep the area closed to visitors and of course that's for visitors' safety," the USS Memorial chief of interpretation said. After a few hours, it was determined the bag belonged to one of the Pearl Harbor survivors. Inside the bag was his oxygen tank. Source: <http://www.hawaiinewsnow.com/Global/story.asp?S=13632519>

POSTAL AND SHIPPING

(Texas) White powder found in mail at local hotel. A suspicious white powdery substance was discovered on the contents of an envelope received in the mail at the Hampton Inn on Texas Avenue in College Station, Texas. The two employees who discovered the envelope December 9 contacted College Station authorities. The envelope and its contents were confined to a small office area. When the first responding unit arrived on the scene, neither of the two persons exposed to the powder were exhibiting any symptoms of exposure to a hazardous substance. EMS personnel kept both employees under observation while hazardous materials response team members entered the office and tested the envelope and its contents. No toxic or hazardous substance was found. Source: [http://www.kbtx.com/local/headlines/White Powder Found in Mail at Local Hotel 111628404.html](http://www.kbtx.com/local/headlines/White_Powder_Found_in_Mail_at_Local_Hotel_111628404.html)

(Massachusetts) White powder sent to BJ's Wednesday poses no threat, says FBI. An envelope sent to the Natick, Massachusetts BJ's Wholesale Club containing a threatening letter and white powder December 8 prompted a state hazmat and FBI response, according to a fire chief. According to preliminary tests, the powder did not pose a risk to employees, said an FBI spokesman. He would not say whether the incident will be further investigated by his agency, per FBI policy. He said an employee got the mail December 8 at about 4:10 p.m., and found the letter and powder. He did not know what the letter said or who sent it. Source: http://www.boston.com/yourtown/news/natick/2010/12/white_powder_sent_to_bjs_veste.html

UPS expands photo ID requirement for retail shipping. United Parcel Service Inc. (UPS) will require customers shipping packages to show government-issued photo identification in an effort to intensify security after explosives were found on October cargo flights. The new policy expands a previous rule in place at UPS Customer Centers to include all retail outlets. Customers without a pre-printed shipping label will have to display an ID, Atlanta-based UPS said in a statement December 7. "Since retail centers experience a significant increase in business from occasional shippers during the busy holidays, this enhancement adds a prudent step in our multilayered approach to security," the vice president of small business and retail marketing said in the statement. Source:

<http://www.bloomberg.com/news/2010-12-07/ups-expands-photo-id-rule-for-retail-shipping-as-bombs-spur-security-steps.html>

Postal service fights counterfeit stamps. As the U.S. Postal Service (USPS) grapples with service cuts and massive budget shortfalls, an estimated \$134.4 million of its annual revenue is quietly slipping away to counterfeiters and perpetrators of other types of postal fraud, FOXNews.com reported December 6. Counterfeit stamps have been identified as a steady, recurring risk for USPS, which reported a loss of \$8.5 billion in the last fiscal year — and they are one of the 10 biggest threats to USPS revenue, according to the 2009 annual report of the U.S. Postal Inspection Service, the law enforcement arm of USPS. Bogus stamps affect the consumers who buy them, too. People who buy stamps online or at local stores are at risk of unknowingly purchasing counterfeits — and then having their mail returned unopened. Source: http://www.myfoxphoenix.com/dpps/news/postal-service-fights-counterfeit-stamps-dpgonc-20101207-fc_10974243

PUBLIC HEALTH

(Arizona) Arizona experiences worst outbreak of West Nile in U.S. A new report shows Arizona experienced the nation's worst outbreak of West Nile virus during this year's season, accounting for nearly one in five severe cases. A total of 159 confirmed cases were reported in Arizona through November 30, according to the Centers for Disease Control (CDC) in Atlanta. At least a dozen Arizonans died. State officials updated the count December 2, reporting 163 cases. Arizona had nearly 20 percent of the nation's neuroinvasive-disease cases. The disease attacks the nervous system and can lead to life-threatening West Nile encephalitis and West Nile meningitis. The spike in Arizona was so severe CDC officials visited in September to study the outbreak. It was mainly concentrated in Gilbert, Chandler, and Tempe, as well as in Pinal County. The CDC is still analyzing the data. Scientists were surprised to see Arizona's urban desert region lead the nation in cases, considering West Nile was thought to be more prevalent in mosquito-rich environments, the manager for the Arizona Department of Health Services' vector-borne disease program said. Source: <http://www.azcentral.com/arizonarepublic/local/articles/2010/12/09/20101209arizona-west-nile-virus-cases.html#ixzz17cKISiW1>

Web-based reporting system creates largest database of medication errors in primary care.

Communication problems and lack of knowledge are the most frequent contributors to medication errors and adverse drug events in primary care practice offices, according to a study of a prototype Web-based Medication Error and Adverse Drug Event Reporting System (MEADERS). The system was developed by investigators from the Regenstrief Institute and Indiana University School of Medicine. The study appears in the November/December 2010 issue of the Annals of Family Medicine. Urban, suburban, and rural primary care practices in California, Connecticut, Oregon, and Texas used MEADERS for 10 weeks, submitting 507 confidential event reports. The average time spent reporting an event was about 4 minutes. Seventy percent of reports included medication errors only. Only 2 percent included medication errors and adverse drug events. The study found medications used for cardiovascular, central nervous system (including pain killers), endocrine diseases (mainly diabetes), and antibiotics were most often associated with events reported in MEADERS. "Our study has created what is now the largest database of medication errors in primary care," said the president and CEO of the Regenstrief Institute. Source: <http://www.healthcareitnews.com/news/web-based-reporting-system-creates-largest-database-medication-errors-primary-care>

(Florida) **Another confirmed case of cholera in Florida.** Miami, Florida health officials said test results confirmed that an American Airlines passenger who became ill on a flight from the Dominican Republic to Miami November 25 had cholera. The Miami-Dade Health Department released the results December 6. Officials said the man was a doctor who had been treating cholera patients. This marks the third confirmed case in Florida. State health officials said a Collier County woman and an Orlando-area woman have recovered from cholera linked to an outbreak in Haiti. Source: <http://www.cbs12.com/news/cholera-4729943-case-haiti.html>

(Georgia) **Georgia tops U.S. in seasonal flu activity.** So far, Georgia is the state hit the hardest by this year's influenza virus, according to the Center for Disease Control and Prevention (CDC). "Georgia is reporting high levels of influenza-like activity," the director of the CDC's National Center for Immunization and Respiratory Diseases said at a December 6 news conference. "It gets a 10 of 10, and is leading the country in terms of what we will be seeing." The flu — largely influenza type B — has been reported throughout Georgia, and been seen mainly in school-aged children, she said. Officials said this year's flu vaccine, which is recommended for everyone older than 6 months, is likely a good match for this year's flu, she said. "Some H1N1, an A/H3N2 strain, and B-strains have been seen this year, [along with] a mixture of B strains and A strains that haven't been characterized," she said. This year's vaccine protects against seasonal flu and the H1N1 swine flu. About 160 million doses of the vaccine have already been distributed nationwide, she said. Source: <http://www.webmd.com/cold-and-flu/news/20101206/georgia-tops-us-in-seasonal-flu-activity>

TRANSPORTATION

(Arkansas) **Independence County man indicted for making bomb.** An Arkansas man was indicted December 7 for making and possessing a bomb. The 20-year-old resident of Magness, Arkansas, was indicted on two counts of unlawfully manufacturing and possessing an improvised explosive device. The indictment also charges that he was both a felon and an unlawful user of a controlled substance at the time he possessed the improvised bomb. According to the United States Attorney for the Eastern District of Arkansas, the suspect is accused of making and planting a bomb on the Dota Creek Bridge near Newark in October 2010. The four-count indictment charges two violations of the National Firearms Act, which carry a possible punishment of up to 10 years in federal prison and/or up to a \$10,000 fine. The felon in possession and unlawful user of a controlled substance charges each have a possible sentence of up to 10 years in federal prison and/or a \$250,000 fine. The suspect is currently being held in the Independence County Detention Center. Source: <http://www.kait8.com/Global/story.asp?S=13634063>

Railroad Research Foundation obtains USDOT grant for TIH routing tool. The U.S. Department of Transportation recently awarded Association of American Railroads affiliate Railroad Research Foundation (RRF) a \$1.5 million Railroad Safety Technology Grant to implement a risk management tool for railroads to comply with federal regulations governing hazardous materials transportation. RRF will use the proceeds to enhance and implement the Rail Corridor Risk Management System, a Web-based software tool designed to analyze the safest, most secure routes to transport certain hazardous materials. The technology is being developed in partnership with the Federal Railroad Administration, Federal Emergency Management Agency, Transportation Security Administration,

UNCLASSIFIED

and the Pipeline and Hazardous Materials Safety Administration. Federal regulations require railroads to conduct ongoing, comprehensive risk analyses of primary routes used to ship certain hazardous materials, as well as alternative routes. The analyses include at least 27 specific risk factors, as well as input provided by state and local governments. Source:

<http://www.progressiverailroading.com/news/article/Railroad-Research-Foundation-obtains-USDOT-grant-for-TIH-routing-tool--25174>

WATER AND DAMS

EPA announces 2010 enforcement and compliance results / More than 1.4 billion pounds of harmful air, land, and water pollution to be reduced. The U.S. Environmental Protection Agency (EPA) announced December 6 the release of its annual enforcement and compliance results. In fiscal year (FY) 2010, EPA took enforcement and compliance actions that require polluters to pay more than \$110 million in civil penalties and commit to spend about \$12 billion on pollution controls, cleanup, and environmental projects that benefit communities. These actions when completed will reduce pollution by more than 1.4 billion pounds and protect businesses that comply with regulations by holding non-compliant businesses accountable when environmental laws are violated. As a result of water cases concluded in FY 2010, EPA is ensuring an estimated 1 billion pounds of water pollution per year will be reduced, eliminated or properly managed and investments in pollution control and environmental improvement projects from parties worth approximately \$8 billion will be made. EPA's criminal enforcement program opened 346 new environmental crime cases in FY 2010. These cases led to 289 defendants charged for allegedly committing environmental crimes, the largest number in 5 years, 198 criminals convicted and \$41 million assessed in fines and restitution. Source: <http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afd88a3852576b3005a604f/78264683b1a9874e852577f10059b840!OpenDocument>

(Connecticut) Computer glitch shuts down water plant. An early morning computer failure December 4 at the First Taxing District's Water Department filtration plant on Valley Road in New Canaan, Connecticut, caused water to flow across the roadway. The plant resumed operating before 8 a.m., the district general manager said. He said residents along Valley Road may find their water discolored, and suggested they let the water run until it clears. The water is safe to drink, he said. A computer shut down in the plant, causing it to stop processing water. However, water continued to be pumped into the building from the adjacent reservoir, eventually causing water to rise up from a manhole and across Valley Road. Source: <http://newcanan.patch.com/articles/computer-glitch-shuts-down-water-plant>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295 (IN ND ONLY); Email: ndslic@nd.gov ; Fax: 701-328-8175
State Radio: 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED